Chairmans draft 6 Dec 84

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE

NO. 1/16[1]

SECURITY OF FOREIGN INTELLIGENCE

IN

Automated ~~COMPUTER~~ SYSTEMS

AND

NETWORKS

(Effective _____)

Pursuant to Section 102 of the National Security Act of 1947, Executive Order 12036, National Security Council (NSC) Directives and to ensure uniform protection of classified foreign intelligence and foreign counterintelligence[2] involving sensitive intelligence sources and methods, processed ~~and/or~~, stored, or Communicated by ~~in~~ computer systems and networks and/or transmitted to or between such systems or networks on telecommunications networks, the following policy and security requirements are hereby established.

The diversity and complexity of computer systems and networks now in operation in the U.S. Intelligence Community and those already designed for future installation may not provide for full compliance with the provisions of the Directive and the attached Automation ~~Computer~~ Security Regulation, therefore, the extent to which the exceptions to this Directive are applied to such systems and networks is left to the determination of each National Foreign Intelligence Board (NFIB) member in view of his ultimate responsibility for the protection of intelligence information.

1. Supercedes DCID 1/16, effective 6 June 1978.

2. Foreign intelligence and counterintelligence are used in this directive as defined in Section 4, Executive Order 12036, and as classified under the provisions of Executive Order 12065. For the purposes of this Directive, the term "intelligence information shall include both foreign intelligence and counterintelligence as so defined.

APPLICABILITY

This Directive shall apply to NFIB members, agencies and all other United States Government departments and agencies which process and/or store intelligence information in computer systems and networks. It shall apply equally when such computer systems and networks are owned and/or operated by the United States Government or by its contractors or consultants.

POLICY

The NFIB members shall establish and maintain a formal security program to ensure adequate protection is provided for intelligence information processed in the community's computer systems and networks. The use of automated systems requires that intelligence information, when processed by computers be afforded protection equivalent to that dictated by Presidential Policy, NSC Directives, Director of Central Intelligence (DCI) Directives and other regulations concerning the overall information security requirements, compartmentation, need-to-know controls, handling caveats, personnel access requirements, and dissemination procedures.

The minimum security requirements for the authorized modes of operation and the recommended criteria for determining whether the specific system or

network provides the required protection is contained in the attached security regulation. The NFIB member(s) concerned may establish for specific system(s) or network(s) additional security measures and capabilities if deemed appropriate. Computer systems involving foreign governments shall be addressed on a case-by-case basis by the NFIB member(s) involved.

This Directive does not supercede or augment the requirements on the control, use, and dissemination of Restricted Data, Fomerly Restricted Data or Communications Security (COMSEC) related material as established by or under existing statutes, directives or Presidential Policy.

AUTHORITY

The NFIB members are assigned the following authority concerning computer/network system accreditations:

System/Network - The NFIB member who is the single user of a system/network is designated the Accreditation Authority for that system/network.

Multiple NFIB Members' System/Network - One NFIB member, selected by those NFIB members involved, will be designated as the Principal Accreditation Authority when a system/network is jointly used by more than one NFIB member.

NFIB Members' Concatenated Systems/Networks - When two or more systems/networks are interconnected or when a system is connected to a network of systems, the NFIB members who are already designated as the Approval Accreditation or Principal Authority of any of the systems/networks involved

Will become a member of the Joint Accreditation Authority for the concatenated systems/networks. One of the NFIB members of the Joint Accreditation Authority will be designated, by joint agreement, Principal Joint Accreditation Authority and all NFIB members shall act as a common body for executing out the responsibilities of the Joint Accreditation Authority.

RESPONSIBILITIES - The NFIB member(s) serving as Accreditation Authorities are responsible to:

a. Assure the most economical and effective utilization of NFIB resources while complying with the stated DCI policy.

b. Identify the information security requirements for the specific system/network based on applicable intelligence information security policies and regulations.

c. Define the complete set of security measures/mechanisms required based on the functionality of the system/network, the user/operational environment, the information characteristics, and applicable information security criteria.

d. Perform the technical assessments, risk analyses and security tests upon which an accreditation of the system/network can be granted.

e. Evaluate the system/network for compliance with this Directive and the standards/criteria established in the accompanying Regulation, and certifying such compliance.

f. Accredit the system/network and establish the allowable operational environment based on the assessment and the security tests of the system/network.

g. Coordinate all system security actions to ensure that all managers

and users of a computer system/network implement the established security measures and capabilities.

EXEMPTIONS - The NFIB member or his designee may temporarily exempt specific systems under his jurisdiction from complete compliance with this Directive and the accompanying Regulation when such compliance would significantly impair the execution of his mission. An exemption shall be granted only when the NFIB member or his designee is assured that the other security measures in effect will adequately protect the intelligence information being processed.

SUPERSESSION - This Directive supersedes Director of Central Intelligence Directive No. 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks", effective 6 June 1978; and all existing directives, regulations, and other documents referencing the superseded Directive.

IMPLEMENTATION - Each NFIB member will develop and promulgate a formal computer security program, implementing directives and regulations within one year from the effective data of this Directive and the accompanying Regulation for systems and networks under his jurisdiction.

ADMINISTRATIVE REPORTS - Each NFIB member or his designee will provide to the Chairman, DCI Security Committee, an annual report as of 31 December detailing the accredited and exempted systems currently operating under his jurisdiction.

REVIEW - This Directive and the accompanying Regulation will be reviewed within three years from the effective date.